STATE OF MICHIGAN

BEFORE THE MICHIGAN PUBLIC SERVICE COMMISSION

* * * * *

In the matter, on the Commission's own motion, to review issues concerning cybersecurity and the effective protection of utility infrastructure.	))))	Case No. U-18203

At the November 22, 2016 meeting of the Michigan Public Service Commission in Lansing, Michigan.

PRESENT: Hon. Sally A. Talberg, Chairman
Hon. Norman J. Saari, Commissioner
Hon. Rachael A. Eubanks, Commissioner

ORDER

History of Proceedings

On January 12, 2012, the Commission opened Case No. U-17000, to address issues and concerns associated with the deployment of advanced metering infrastructure (AMI) by Michigan electric utilities. In the January 12 order, the Commission directed all regulated electric utilities to file information in the docket concerning various aspects of AMI. In addition, the Commission requested written comments from interested parties and directed the Commission Staff (Staff) to prepare a report addressing the utility filings, comments from the public, and other pertinent information. On June 29, 2012, the Staff submitted its report (Staff Report), and on October 12, 2012, the Commission issued an order in which it found, *inter alia*, that cybersecurity issues were of sufficient complexity and importance to merit the establishment of this docket.[1] Further, in two recent rate case proceedings, the Commission directed DTE Electric Company (DTE Electric) and

[1] The Commission addressed customer data privacy in various orders issued in Case No. U-17102.

Consumers Energy Company (Consumers) to each provide the Staff with periodic reports on the utility's cybersecurity program. *See,* November 19, 2015 order in Case No. U-17735, p. 18, and December 11, 2015 order in Case No. U-17767, p. 116. In those cases, the Staff provided a general framework outlining the type and scope of cybersecurity information to be provided to the Commission.

Discussion

As reviewed at length in the Staff Report, cybersecurity is critical to the operation of a modern electric utility and utilities must continually assess and upgrade their defenses to cyber attacks. While the Commission recognizes that AMI itself could increase the vulnerability of the electric grid, grid automation generally, including the deployment of a number of "smart" grid components, inherently increases the risk to system security. Increased security risks arise largely, but not exclusively, because grid modernization involves increasing the number of digital access points within the electric distribution system and increasing the number of and level of control by networked devices.

According to the Staff Report, p. 14:

> As Michigan transitions to a more technologically advanced power grid, it is important that the proper actions are taken by utilities to address cyber security threats. Cyber security planning is defined as preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. The attention cyber security has received at the national and state levels for many years indicates that utilities, regulators and consumers all share common concerns. Improving the electrical grid involves gathering more data and utilizing more technology. With every added piece of technology, the risk of vulnerabilities inherently increases. The U.S. [Department of Energy] DOE has stated that the smart grid of the future should be secure and resilient against all forms of attacks. A smarter grid includes more devices and connections that may become avenues for intrusions, error-caused disruptions, malicious attacks, destruction, and other threats. (Internal citations omitted.)

The Commission has a duty to ensure that public utility companies provide safe and adequate service at just and reasonable rates. Because cybersecurity threats challenge the reliability, resiliency, and safety of the electric grid, and because utility spending to address cyber vulnerabilities can impact the bills that customers pay, the Commission has an obligation to fully examine utilities' cybersecurity practices. In addition, because most gas transportation and distribution systems rely extensively on supervisory control and data acquisition (SCADA) for gas system monitoring and control, these systems also require cybersecurity protections.

Given the concerns about cybersecurity, critical infrastructure, and the need for uniformity in reporting among regulated utilities, the Commission directs the Staff to craft rules to be included in the Technical Standards for Electric Service, Mich Admin Rule 460.3101 *et seq.* and in the Technical Standards for Gas Service, Mich Admin Rule 460.2301 *et seq.* The rules shall provide for an annual report that includes an overview of the electric or gas provider's cybersecurity program; a list of the company's cybersecurity departments, staffing numbers and position descriptions, and the names of key contacts; a description of any cybersecurity training and exercises undergone by employees; an explanation of any cybersecurity investment made and the rationale for such investment; a discussion of the tools and methods used to conduct risk and vulnerability assessments; and a summary of cybersecurity incidents that resulted in a loss of service, financial harm, or a breach of sensitive business or customer information.

THEREFORE, IT IS ORDERED that the Commission Staff shall draft and include rules concerning cybersecurity reporting in amendments to the Technical Standards for Gas Service and Technical Standards for Electric Service.

The Commission reserves jurisdiction and may issue further orders as necessary.

MICHIGAN PUBLIC SERVICE COMMISSION

_____

Sally A. Talberg, Chairman

_____

Norman J. Saari, Commissioner

_____

Rachael A. Eubanks, Commissioner

By its action of November 22, 2016.

_____

Kavita Kale, Executive Secretary